# Cisco Finesseリバースプロキシによる Finesseデスクトップへの VPNレスアクセスにおける DoS脆弱性

| | | |
|---|---|---|
| Medium | **アドバイザリーID :** cisco-sa-finesse-proxy-dos-vY5dQhrV<br>**初公開日 :** 2023-03-01 16:00<br>**最終更新日 :** 2023-03-02 20:35<br>**バージョン 1.1 :** Final<br>**CVSSスコア :** 5.3<br>**回避策 :** Yes<br>**Cisco バグ ID :** CSCwd67008 | CVE-2023-20088 |

**日本語による情報は、英語による原文の非公式な翻訳であり、英語原文との間で内容の齟齬がある場合には、英語原文が優先します。**

## 概要

Cisco FinesseのVPNレス逆プロキシの一部として提供されるnginx設定の脆弱性により、認証されていないリモートの攻撃者が、ロードバランサを介して接続する新規および既存のユーザに対してサービス妨害(DoS)状態を作成する可能性があります。

この脆弱性は、逆プロキシによる不適切なIPアドレスフィルタリングに起因します。攻撃者は、認証されていない一連の要求をリバースプロキシに送信することで、この脆弱性を不正利用する可能性があります。エクスプロイトに成功すると、攻撃者は現在のすべてのトラフィックと、ロードバランサを経由するリバースプロキシへの後続の要求をドロップさせ、DoS状態を引き起こす可能性があります。

シスコはこの脆弱性に対処するソフトウェアアップデートをリリースしています。本脆弱性に対処する回避策がいくつかあります。

このアドバイザリは、次のリンクより確認できます。
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-finesse-proxy-dos-vY5dQhrV

## 該当製品

### 脆弱性のある製品

公開時点で、この脆弱性がCisco Finesseに影響を与えたのは、リバースプロキシがインストールされ、リバースプロキシへの要求がロードバランサを介してルーティングされた場合だけです。

Cisco Finesseにバンドルされている次のシスコ製品も、この脆弱性の影響を受けます。

- Packaged Contact Center Enterprise(PCCE)
- Unified Contact Center Enterprise（UCCE）
- Unified Contact Center Express（UCCx）

公開時点で脆弱性が確認されている Cisco ソフトウェアのリリースについては、このアドバイザリの「修正済みソフトウェア」セクションを参照してください。最も完全で最新の情報については、このアドバイザリの上部にあるバグ ID の詳細セクションを参照してください。

### 脆弱性を含んでいないことが確認された製品

このアドバイザリの脆弱性のある製品セクションに記載されている製品のみが、この脆弱性の影響を受けることが分かっています。

## 回避策

この脆弱性の回避策は、修整版リリースにアップグレードできないお客様に使用できます。回避策の実装の調整に関しては、 Cisco Technical Assistance Center（TAC）にお問い合わせください。

この回避策は導入されており、テスト環境では実証済みですが、お客様は、ご使用の環境および使用条件において適用性と有効性を判断する必要があります。また、導入されている回避策または緩和策が、お客様固有の導入シナリオおよび制限に基づいて、ネットワークの機能やパフォーマンスに悪影響を及ぼす可能性があることに注意してください。回避策や緩和策は、ご使用の環境への適用性と環境への影響を評価した後で導入してください。

## 修正済みソフトウェア

ソフトウェアのアップグレードを検討する際には、シスコ セキュリティ アドバイザリ ページで入手できるシスコ製品のアドバイザリを定期的に参照して、侵害を受ける可能性とアップグレード ソリューション一式を確認してください。

いずれの場合も、アップグレードするデバイスに十分なメモリがあること、および現在のハードウェアとソフトウェアの構成が新規リリースで引き続き正しくサポートされていることを十分に確認してください。不明な点については、Cisco Technical Assistance Center（TAC）もしくは契約しているメンテナンスプロバイダーにお問い合わせください。

発行時点では、次の表に示すリリース情報は正確でした。最も完全で最新の情報については、こ

のアドバイザリの上部にあるバグ ID の詳細セクションを参照してください。

左側の列にはシスコソフトウェアリリース、右側の列にはリリースがこのアドバイザリに記載されている脆弱性の影響を受けるかどうか、およびこの脆弱性に対する修正を含むリリースが示されています。

| Cisco Finesseリリース | First Fixed Release ( 修正された最初のリリース ) |
|---|---|
| 12.6(1) ES7より前 | 12.6(1) ES7 |

修正済みリリースのインストールに加えて、リバースプロキシおよびロードバランサなどの中間デバイスに次の設定を適用する必要があります。

- ロードバランサなどのリバースプロキシのフロントエンドを担う中間ネットワークデバイスは、不正ユーザのIPアドレスではなくリバースプロキシのIPアドレスをブロックしないように、レート制限や不正アクセスのブロックを目的とした設定から除外する必要があります。これらのデバイスを正しく設定するには、『Cisco Unified Contact Center Enterprise機能ガイド、リリース12.6(1) – リバースプロキシ設定』のステップ1に従います。
- リバースプロキシのフロントエンドを担う中間ネットワークデバイス ( ロードバランサなど ) は、中間デバイスのIPアドレスの代わりにユーザのIPアドレスを要求に含めることができる機能を有効にする必要があります。これらのデバイスを正しく設定するには、『Cisco Unified Contact Center Enterprise機能ガイド、リリース12.6(1) – リバースプロキシ設定』のステップ2および3を実行します。

Product Security Incident Response Team ( PSIRT; プロダクト セキュリティ インシデント レスポンス チーム ) は、このアドバイザリに記載されている該当するリリース情報と修正されたリリース情報のみを検証します。

## 不正利用事例と公式発表

Cisco PSIRT では、本アドバイザリに記載されている脆弱性の不正利用事例やその公表は確認しておりません。

## 出典

この脆弱性は Cisco TAC サポートケースの解決中に発見されました。

## URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-finesse-proxy-dos-vY5dQhrV

## 改訂履歴

| バージョン | 説明 | セクション | ステータス | 日付 |
| --- | --- | --- | --- | --- |
| 1.1 | 脆弱性が存在するリリースを明確にした。 | 修正済みリリース | Final | 2023年3月2日 |
| 1.0 | 初回公開リリース | - | Final | 2023年3月1日 |

# 利用規約

本アドバイザリは無保証のものとしてご提供しており、いかなる種類の保証も示唆するものではありません。 本アドバイザリの情報およびリンクの使用に関する責任の一切はそれらの使用者にあるものとします。 また、シスコは本ドキュメントの内容を予告なしに変更したり、更新したりする権利を有します。
本アドバイザリの記述内容に関して情報配信の URL を省略し、単独の転載や意訳を施した場合、当社が管理した情報とは見なされません。そうした情報は、事実誤認を引き起こしたり、重要な情報が欠落していたりする可能性があります。 このドキュメントの情報は、シスコ製品のエンドユーザを対象としています。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。